科来

第 28 章
如何定位引起网络丢包的根源

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

网络丢包通常是比较难排查的问题，因为造成网络丢包的原因很多，排查此类问题需要很长的时间。本案例中，通过对网络通信数据进行比对分析，从而找到引起网络丢包的问题根源。

28.1 问题描述

可编程逻辑控制器（PLC），是一种采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械或生产过程。PLC 实质是一种专用于工业控制的计算机。

某集团公司 PLC 设备近期出现异常，设备经常报告连接故障，公司网络运维人员通过 Ping 测试发现该设备存在丢包现象（丢包率约 1~2%）。为了寻找问题原因，避免再次出现类似问题，在科来网络分析工程师的协助下，在出问题的 PLC 设备接入交换机处旁路部署了科来网络回溯分析系统进行数据包级分析。PLC 网络环境及分析设备部署示意图如下。

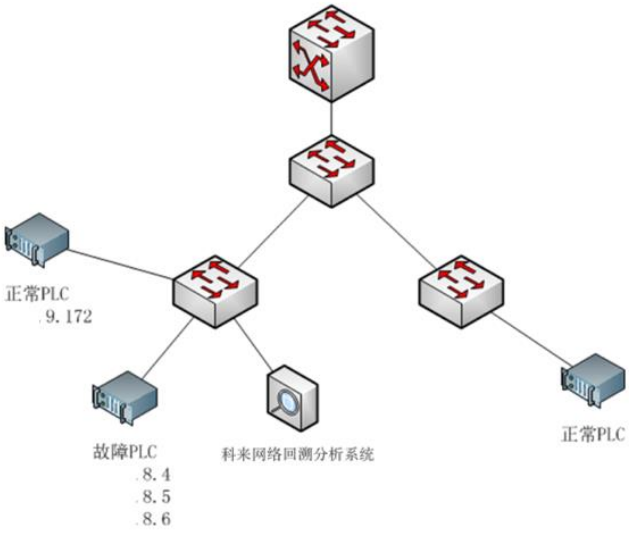


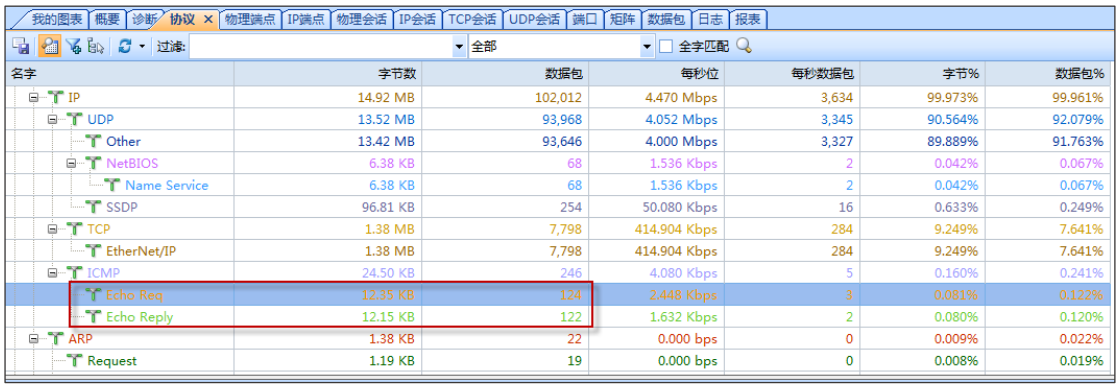
图 28-1

通过交换机端口双向流量镜像分别采集故障 PLC 和正常 PLC 的通信数据进行比对分析，以下是详细分析过程及分析结论。

28.2 分析过程

28.2.1 故障 PLC 单网卡数据分析

首先，我们镜像故障 PLC 问题最严重网卡（IPX.X.8.4）的接口双向流量，在采集数据的同时，公司技术人员配合从核心交换机处 ping“X.X.8.4”。从采集到的 ICMP 协议报文数量可以看到：测试期间共捕获 124 个 ping 请求包（Echo Req），但只捕获 122 个 ping 应答包（Echo Reply），如下图所示。



名字	字节数	数据包	每秒位	每秒数据包	字节%	数据包%
IP	14.92 MB	102,012	4.470 Mbps	3,634	99.973%	99.961%
UDP	13.52 MB	93,968	4.052 Mbps	3,345	90.564%	92.079%
Other	13.42 MB	93,646	4.000 Mbps	3,327	89.889%	91.763%
NetBIOS	6.38 KB	68	1.536 Kbps	2	0.042%	0.067%
Name Service	6.38 KB	68	1.536 Kbps	2	0.042%	0.067%
SSDP	96.81 KB	254	50.080 Kbps	16	0.633%	0.249%
TCP	1.38 MB	7,798	414.904 Kbps	284	9.249%	7.641%
EtherNet/IP	1.38 MB	7,798	414.904 Kbps	284	9.249%	7.641%
ICMP	24.50 KB	246	4.080 Kbps	5	0.160%	0.241%
Echo Req	12.35 KB	124	2.448 Kbps	3	0.081%	0.122%
Echo Reply	12.15 KB	122	1.632 Kbps	2	0.080%	0.120%
ARP	1.38 KB	22	0.000 bps	0	0.009%	0.022%
Request	1.19 KB	19	0.000 bps	0	0.008%	0.019%

图 28-2

可以看出从故障 PLC 设备到边缘交换机接口就存在丢包现象，故障 PLC 有 1.6%的包没有传输到边缘交换机。同时，在测试期间 X.X.8.4 的 TCP 通信中存在明显的丢包现象，如下图所示。

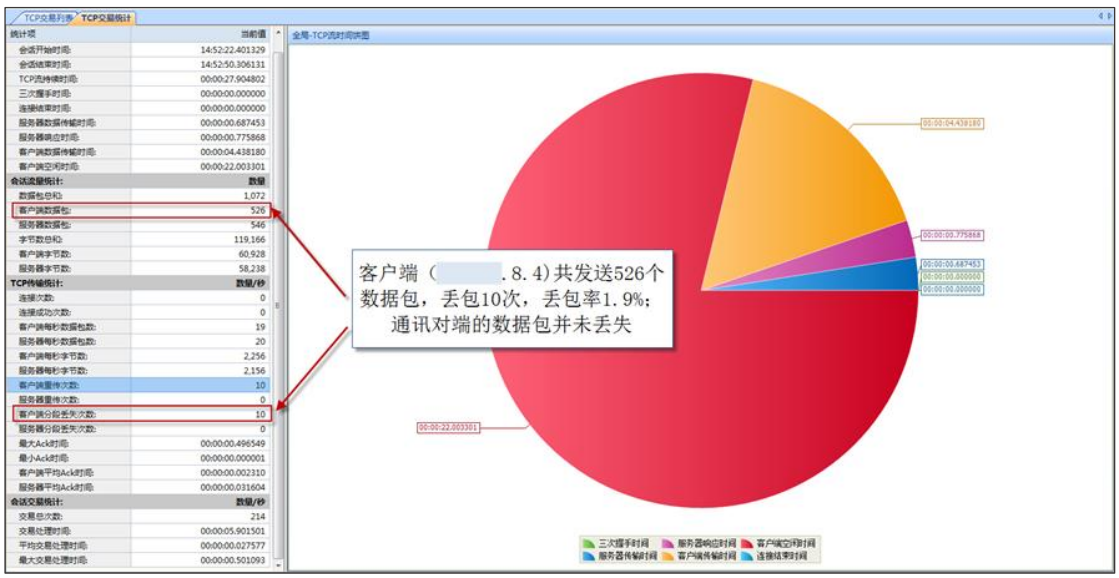


图　28-3

通过以上数据，我们可以初步判断造成丢包现象的原因出自故障 PLC 到接入交换机之间，可能的问题点包括：

接入交换机接口故障；

故障 PLC 接入网线故障；

故障 PLC 设备自身网卡或其他硬件故障。

28.2.2　故障 PLC 全部网卡数据分析

第二步，我们镜像了故障 PLC 的全部三个网卡连接的交换机接口双向流量，发现三个网卡都有丢包现象，而且丢包量基本相当，如下图所示。

图　28-4

这说明丢包并不是 X.X.8.4 一个网卡的问题，而是故障 PLC 三个网卡的都有的现象。从其 TCP 会话统计来看也都是从 PLC 设备发送到接入交换机时出现的丢包。

由于三个网线或三个交换机接口同时存在问题的可能性很小，所以我们基本可以判断是故障 PLC 设备自身硬件问题导致的丢包现象。

28.2.3　正常 PLC 数据分析

第三步，我们镜像在同一边缘交换机的正常 PLC 设备（X.X.9.172）接口的流量，从采集数据中我们只看到了很少量的 TCP 重传，并且这些重传都是与 X.X.8.4 相关的通讯导致的，如下图所示。

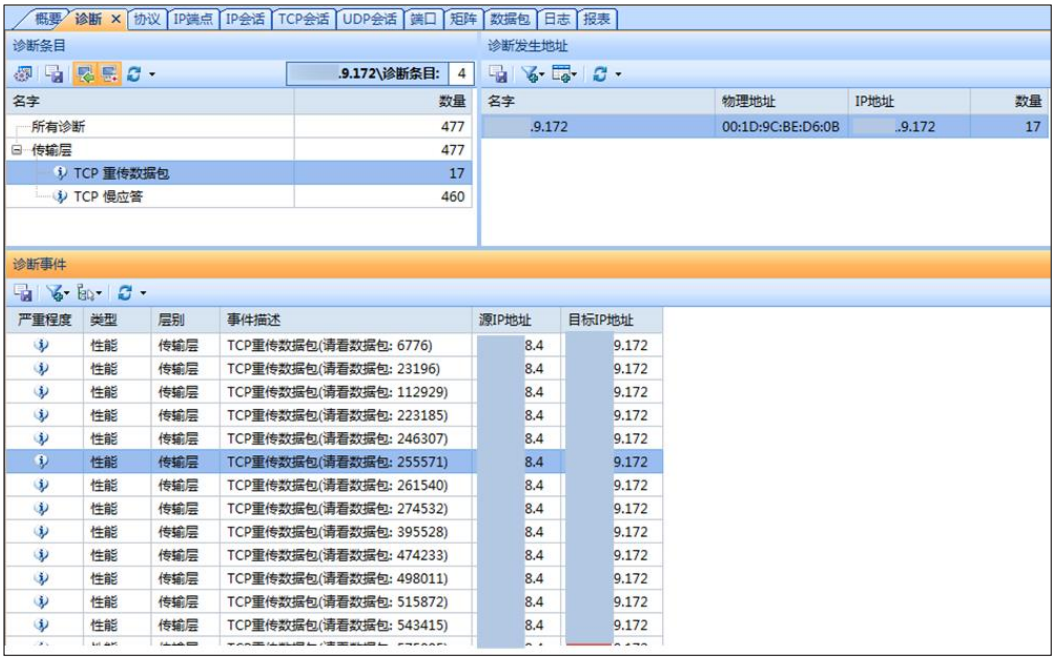


图　28-5

这说明正常 PLC 设备到接入交换机之间并没有明显的丢包迹象，进一步验证了之前的分析结论。

28.3　分析结论

通过以上数据分析，我们判断存在丢包问题的 PLC 设备极有可能是由于设备自身硬件问题，导致数据包没有正常的从网卡发送到网络中所致；网线和接入交换机接口导致丢包现象的可能性非常小。

建议用户在非生产时段用 PC 机接入到故障设备的网线上，配置相同 IP 地址，通过 ping 测试是否还存在丢包现象，如果没有出现丢包或丢包率远小于 1%即可完全排除网络原因。

28.4　价值

通过网络分析技术对传输的数据流进行深入分析，可从多种可能原因中快速定位问题根源，使网络丢包不在困扰网络管理员。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统(UPM)
- 科来网络回溯分析系统(RAS)
- 科来网络分析系统(CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台(BAP)
- 科来网络全流量安全分析系统(TSA)
- 科来APT攻击检测系统(APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区